



Department of Homeland Security Daily Open Source Infrastructure Report for 17 August 2005

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Albuquerque Tribune reports Arizona Governor Janet Napolitano has joined New Mexico Governor Bill Richardson in declaring a state of emergency along her state's border with Mexico. (See item [13](#))
- The Associated Press reports U.S. Department of Agriculture inspectors have found more than 1,000 violations of rules aimed at preventing mad cow disease from reaching humans. (See item [17](#))
- Yale University reports Yale School of Medicine has launched a database containing scientific evidence about how animal disease events can be an early warning system for emerging human diseases. (See item [23](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) –

<http://www.esisac.com>]

1. *August 16, Interstate Renewable Energy Council USA* — **New Connecticut law requires utilities to use distributed generation.** Connecticut has enacted legislation that will significantly promote and facilitate the development of distributed generation (DG) in the state. HB 7501, signed into law July 21, 2005, requires electric companies and competitive suppliers to acquire 1% of their supply from DG in 2007, increasing to 4% by 2010. If a company,

supplier or wholesaler does not meet the standard, it must pay \$0.055 for each kilowatt-hour (kWh) of its shortfall. The Connecticut Department of Public Utility Control (DPUC) must complete a contested case by February 1, 2006, to specify the administrative process and specifications for this requirement. DG resources are renamed "grid side distributed resources" in the new law, which expands the definition to include conservation and load management, including peaking reducing and demand-response systems. Distributed resources may not exceed 65 megawatts (MW) in capacity and must be connected to the transmission or distribution grid.

HB 7501: http://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?seIBillType=Bill&bill_num=7501&which_year=2005&SUBMIT.x=10&SUBMIT.y=13

Source: http://www.irecusa.org/articles/static/1/1123616339_98709645_0.html

2. *August 16, Journal News (NY)* — **Nuclear power plant sirens fail a third time.** For the third time in less than a month, the four-county emergency siren system at the Indian Point nuclear plant, located in Buchanan, NY, did not work properly on Monday, August 15, the result of telephone line problem, Westchester and Rockland County, NY, officials said. A spokesperson for Indian Point's owner, Entergy Nuclear Operations, said that, despite the problem, the sirens themselves could have been activated from the plant if needed. About 9:15 a.m. Monday, emergency officials in Rockland County ran a silent test regularly done on Mondays to make sure the 156-siren system was performing properly. When the test showed a network failure, Rockland officials contacted Indian Point officials, who were unaware of the problem, said Dan Greeley, Rockland's deputy commissioner for emergency services. Greeley said the problem appeared to be with a Verizon telephone line, a relay point that connects the four counties and the siren network with Indian Point via computers.

Source: <http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20050816/NEWS02/508160324/1017>

3. *August 16, The Honolulu Advertiser* — **Nanakuli fire sweeps valley, threatens power plant.** Firefighters struggled on Monday, August 15, to contain a frustrating brushfire that had burned more than 2,000 acres in Nanakuli, HI, closing schools and roads. Late Monday night, crews scrambled to the Kahe power plant, where the fire had flared again, said Hawaii Fire Department spokesperson Captain Emmit Kane. The fire was also near diesel storage tanks at the power plant, but they apparently were in no immediate danger, he said. Around 10:30 p.m. the flames were so bright behind the power plant that it looked like the sun was coming up over the ridge. "This one is pretty much getting close to either eclipsing or surpassing the biggest fire this year," Kane said. "It's requiring a lot of resources and also hindering the response time for other parts of the island. This fire is far from being controlled," he said. The fire started at about 1:30 p.m. Sunday, August 14, about 200 yards from the ridge line on the west facing hillside of Nanakuli Valley. Kane said power lines running from the valley floor to the top of the ridge are being looked at as possible ignition sources.

Source: <http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=/20050816/NEWS01/508160333/1001/NEWS>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

4. *August 16, The Times–Picayune (LA)* — **Sulphur leak at refinery causes a wave of headaches and nausea to local residents.** A strong sulfur odor emanated from the Murphy Oil USA refinery in Meraux, LA, on Monday, August 15, after a sulfur–processing unit failed, causing an undetermined amount of sulfur dioxide to be diverted to the flare system. Neighboring residents complained of nausea and headaches, but there were no reports of serious injury from the release, which authorities said was not a health risk. The sulfur unit shut down about 1 p.m. and was back on line by 3 p.m., said refinery spokesperson Carl Zornes, who on Monday afternoon did not know how much sulfur dioxide was sent to the flare or why the unit shut down. The burned gas produces a strong odor that is irritating but not harmful, Fire Chief Thomas Stone said. Firefighters used fans to ventilate the St. Bernard Parish Health Unit and Mental Health Center on Palmisano Boulevard, where the odor was particularly strong, he said. The incident will be reported to the state Department of Environmental Quality, Zornes said.

Source: <http://www.nola.com/news/t-p/stbernard/index.ssf?/base/news-2/1124174340274310.xml>

5. *August 15, Associated Press* — **Oil tanker overturns in Idaho, spills into river.** An oil tanker overturned on Idaho Highway 55 Monday evening, August 15, spilling an estimated 19 hundred gallons of oil. The Idaho State Police (ISP) says an estimated 200 gallons of oil went into the Payette River, but all of it was believed to be contained. ISP spokesperson Doug Jensen says Hazmat crews from ISP, Valley County, ID, Sheriff's Office, the Bureau of Reclamation and the Boise Regional Response Team were working through the night to try to clean up the spill. Few details were available about what may have caused the crash about 14 miles south of Cascade, ID. Police did not release the name of the driver, but said the truck was owned by Idaho Asphalt. No one was injured in the accident. Jensen says the wreck is expected to keep the northbound lane of Idaho 55 closed until sometime Tuesday morning, August 16.

Source: <http://www.kbcitv.com/x5154.xml?ParentPageID=x5155&ContentID=x17587&Layout=KBCI.xsl&AdGroupID=x5154&URL=http://localhost/apwirefeed/d8c0nhs80.xml&NewsSection=StateHeadlines>

6. *August 14, Associated Press* — **Fire put out at BP plant; cause being investigated.** A small fire that followed an explosion in a plastics manufacturing unit was extinguished and investigators prepared Saturday, August 13, to investigate the cause of the blast at BP's Chocolate Bayou plant near Alvin, TX. The fire was put out late Friday night, August 12, said company spokesperson Dan Cummings. No one was injured in the Wednesday, August 10, explosion and fire in the unit, which produces plastic materials such as ethylene and polypropylene. The plant is located in a remote area about 40 miles south of Houston, TX, is operated by BP subsidiary Innovene. The blast occurred the same day that a heavy oil and gas leak occurred at another BP facility in Texas City, TX. The leak caused a plume of smoke to rise over the area and prompted officials to order nearby residents to stay inside. An explosion at the Texas City plant in March killed 15 people and injured scores of others.

Source: http://www.woai.com/news/state/story.aspx?content_id=04A992BA-CE62-49BE-826B-6B143EB3DE5C

[[Return to top](#)]

Defense Industrial Base Sector

Nothing to report.

[[Return to top](#)]

Banking and Finance Sector

7. *August 16, Expatica News (Netherlands)* — **Online banking hacker arrested in Belgium.**

Self-confessed online banking hacker Pieter Miclotte has been arrested on charges of fraud. Miclotte reported to police in Ghent, Belgium, on Friday, August 12, just hours after Belgian media quoted him saying that thieving via online banking is as easy as plundering a shop with its doors open. He told a newspaper that he'd robbed customers of two banks, namely ING and Keytrade, via online banking. He claimed to have stolen thousands of euros in recent weeks. Miclotte said he gained access during chat sessions to the computers of other online chatters and went looking for information about their banking and bank access codes. He allegedly used those codes to transfer large sums of money to his own accounts.

Source: http://www.expatica.com/source/site_article.asp?subchannel_id=48&story_id=22817&name=%27Home+banking+hacker%27+arrested+in+Ghent

8. *August 15, Department of Justice* — **Massachusetts man sentenced to prison for identity theft in bank scam.** Duykhoa Nguyen, of Auburn, MA, who was formerly employed by Sovereign Bank, in Worcester, MA, was sentenced on Friday, August 12, 2005, for his role in a scheme that involved selling the personal identity information of bank customers that allowed others to gain access to the customers' funds. Nguyen was sentenced by U.S. District Judge Nathaniel M. Gorton to nine months in prison and ordered to pay \$185,000 in restitution to the bank for his role in the conspiracy. Nguyen pleaded guilty on February 12, 2004 to one count of conspiracy and one count of bank fraud. At the earlier plea hearing the prosecutor told the court that, had the case proceeded to trial, the government would have proven that Nguyen, a Senior Personal Banking Representative at Sovereign Bank, agreed to sell to another individual, customer account information, including: names, account numbers, and dates of birth. After Nguyen passed the account information along, others obtained fraudulent identification documents in the names of the Sovereign customers. Subsequently, at Sovereign branches in Connecticut and Rhode Island, imposters used the fraudulent identification documents to withdraw approximately \$185,000 from several Sovereign customers' accounts. In exchange, Nguyen received 10% of the money taken from the accounts.

Source: <http://www.usdoj.gov/usao/ma/presspage/Aug2005/Nguyen-Duykhoa-Sentencing.htm>

[[Return to top](#)]

Transportation and Border Security Sector

9. *August 16, USA TODAY* — **TSA hopes modifications will make X-rays not so revealing.**

The revealing X-ray machines that the federal government wants to use on airline passengers are getting a makeover. The Transportation Security Administration (TSA) is paying two manufacturers to develop ways to expose weapons but conceal body parts. The machines bounce low-radiation X-rays off a person's skin to produce photo-like computer images of

metal, plastic, and organic materials hidden under clothes. They have the potential to detect all weapons on passengers, including plastic knives and explosives that won't set off the metal detectors now used at airport checkpoints. But the American Civil Liberties Union calls them "a virtual strip search." The TSA now hopes to test modified "backscatter" machines in a few airports this fall that will solve the privacy issue. That's a "significant software challenge" because wiping out body parts also makes weapons less visible, says Peter Kant, a vice president at backscatter maker Rapiscan Systems. TSA technology chief Clifford Wilke told a Congressional hearing last month that the altered backscatter images would show a body's outline or silhouette and any objects someone is carrying. If the TSA finds the machines provide adequate privacy and security, it will test them only on passengers getting a second round of screening.

Source: http://www.usatoday.com/travel/news/2005-08-15-tsa-xrays_x.htm

10. *August 16, USA TODAY* — Delta to sell regional carrier Atlantic Southeast Airlines.

Struggling to raise cash in a financial crisis, Delta Air Lines said Monday, August 15, it's selling its Atlanta-based regional carrier, Atlantic Southeast Airlines, to SkyWest for \$425 million. But Delta, the country's No. 3 airline, said in a securities filing Monday that the sale might not forestall an overwhelming cash crunch amid record fuel prices. The acquisition of ASA nearly doubles the size of Utah-based SkyWest, which already flies for Delta as a feeder airline under contract at its Salt Lake City hub. Delta and SkyWest said Monday the deal will mean no significant changes in the flight schedules or cities served by Atlanta-based ASA. Under SkyWest's ownership, ASA's regional jets will continue to feed Delta's larger jet flights from Atlanta. Delta said proceeds from the ASA deal will help pay down \$100 million in outstanding debt to General Electric Commercial Finance and others. If Delta is forced into Chapter 11 this fall, it would need to raise bankruptcy financing, possibly from GE and other lenders that have lent to Delta in the past.

Source: http://www.usatoday.com/travel/news/2005-08-15-delta-shares_x.htm

11. *August 16, CNN* — Venezuela jet crash kills at least 160. A Colombian airliner carrying 160 people crashed Tuesday, August 16, in a remote area of western Venezuela, aviation officials said. No survivors have been found. A spokesperson for West Caribbean Airways, based in Medellin, Colombia, told CNN there were 152 passengers and eight crew members on board, making it the deadliest plane crash in Venezuela's history. The MD-82 aircraft left Tocumen International Airport south of Panama City around 1 a.m. local time, headed for Fort de France, Martinique, according to Panamanian aviation officials. The flight had been chartered by tourists in Martinique, a French possession in the Caribbean. Venezuelan officials said the jetliner's pilots reported engine problems shortly before contact was lost with the aircraft around 3 a.m. ET. The McDonnell Douglas MD-80 series has been involved in 11 fatal crashes since it went into service in 1980 — seven involved the MD-82 model. Boeing acquired McDonnell Douglas in 1997 and ended production of the MD-80 series in 1999. The plane is still in use around the world. The two companies built 1,191 MD-80s.

Source: <http://www.cnn.com/2005/WORLD/americas/08/16/venezuela.crash/index.html>

12. *August 16, Associated Press* — Authorities believe immigrant smugglers have shifted routes.

Nearly a third of the dead illegal aliens found this year perished in a 45-mile stretch from Three Points to the Arizona-Sonora border, leaving investigators to conclude smugglers have shifted their routes to the eastern side of the Baboquivari Mountains 50 miles from

Tucson. Neither the Mexican Consulate nor the U.S. Border Patrol keeps track of how many of the more than 200 bodies found this federal fiscal year in Arizona were reported by citizens but both agencies acknowledge many calls come from private citizens and Mexican citizens who sneaked across the border. Apprehensions of illegal aliens in the Border Patrol's Tucson station, which covers this stretch of Arizona desert, grew by 60 percent. The agency's Nogales station, which shares the area, saw arrests drop by four percent, said sector spokesperson Andrea Zortman. The two stations cover 53 miles of the sector's 280 miles of border with Mexico, and so far are responsible for more than a third of the 390,575 apprehensions made between the start of the fiscal year October 1, 2004 and Thursday, August 11.

Source: <http://kvoa.com/Global/story.asp?S=3720925&nav=HMO6dOFq>

13. *August 16, Albuquerque Tribune (NM)* — Arizona joins New Mexico's efforts at the border.

Arizona Governor Janet Napolitano has joined New Mexico Governor Bill Richardson in declaring a state of emergency along her state's border with Mexico. The order releases \$1.5 million in emergency money for counties that lie along the border. Jeanine L'Ecuyer, a spokesperson for the governor, said the money is intended for use by counties and municipalities to cover overtime pay for law enforcement officers, repairs of border fences and costs related to illegal immigrants' deaths. Richardson said he had to declare the emergency, which provides \$1.75 million in state and federal funding for additional law enforcement along the border. "We're talking about a violent situation," he said between appearances. "We're talking about illegal drugs coming in. We're talking about kidnapping. We're talking about police being shot at. We're talking about a violent situation that has to be dealt with. Something like this is a wake-up call to the Congress that they need a federal immigration policy. They need to deal with issues of legal migration." Mexico President Vicente Fox said Monday that violence along the border makes the need for a migration accord with the United States more urgent.

Source: http://www.abqtrib.com/albq/nw_local/article/0,2564,ALBQ_198_58_4006214,00.html

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

- 14. *August 16, Agricultural Research Service* — Cotton DNA database launched to help find plant resistance.** The Agricultural Research Service (ARS) has joined Cotton Incorporated and Clemson University Genomics Institute Tuesday, August 16, in launching the Cotton Microsatellite Database. Unlike other major crops, cotton did not have a publicly available database for DNA markers. Lack of markers and maps has been a major limiting factor in the development of DNA-based tools to identify important agronomic traits and facilitate selection of plants based on these traits. DNA markers are small pieces of DNA that vary in length, depending on the plant's genetic make-up. When a specific marker is associated with a gene governing resistance to a specific pest or disease, it can be used as a diagnostic tool to identify

plants with potential resistance. This is only the first step toward developing a DNA marker database and creating a map of the cotton genome.

Cotton database: <http://www.mainlab.clemson.edu/cmd>

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

15. *August 16, KFYR (ND)* — **Anthrax toll rises.** The deputy state veterinarian says more than 300 animals in 12 North Dakota counties have died from anthrax. Beth Carlson says it's the largest outbreak the state has ever seen and she says it does not appear to be over. The disease was first found July 6, in a bison herd in Ransom County. State Agriculture officials say 38 farms in that county have been hit.

Source: <http://www.kfyrtv.com/showNews.asp?whatStory=4051>

16. *August 15, Stop Soybean Rust News* — **First soybean rust found in South Carolina.** Soybean rust has been confirmed in the southern part of South Carolina in a Hampton County commercial soybean field. This is the first confirmed rust in the state and becomes the northern-most county with rust in the U.S., just a bit north of Effingham County right across the border in Georgia. Hampton County Extension agent Tommy Walker collected the sample last week, and it was allowed to incubate before being examined on Saturday, August 13. John Mueller, Extension soybean pathologist with Clemson University, pegged it as rust and sent it to the Plant Problem Clinic for confirmation early Monday, August 15. In Mueller's commentary, he said rust in the Hampton County field is at a low level and is doing very little damage to that field, while also not producing enough spores to immediately threaten nearby fields.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=504>

[[Return to top](#)]

Food Sector

17. *August 16, Associated Press* — **Plants cited for mad cow offenses.** Inspectors have found more than 1,000 violations of rules aimed at preventing mad cow disease from reaching humans, the U.S. Department of Agriculture (USDA) said. No contaminated meat reached consumers, the agency said. The rules were created in response to the nation's first case of mad cow disease in December 2003. They require that brains, spinal cords and other nerve parts — which can carry mad cow disease — be removed when older cows are slaughtered. The at-risk tissues are removed from cows older than 30 months because infection levels are believed to rise with age. The USDA said Monday, August 15, it had cited beef slaughterhouses or processing plants 1,036 times for failing to comply with rules on removing those tissues, which are commonly called specified risk materials or SRMs. The violations occurred over 17 months, ending in May 2005. The number of violations amounts to less than one percent of all citations at those plants, said USDA spokesperson Lisa Wallenda Picard.

Source: <http://www.cbsnews.com/stories/2005/08/16/health/main781020.shtml>

18. *August 16, Korea Times* — **Korea to keep U.S. beef away this year.** South Korea is likely to delay the resumption of U.S. beef imports until next year due to some technical problems in proving its safety from mad cow disease or bovine spongiform encephalopathy (BSE), the

Ministry of Agriculture and Forestry (MOAF) said Tuesday, August 16. The Korean government has requested information from the U.S. on the second BSE case reported there in June, but it has not arrived, ministry officials said. "The government plans to convene a meeting of animal disease experts to decide on the resumption of beef imports but the meeting has been postponed due to a delay in the arrival of the requested information," MOAF official Kim Chang-sup said. "We expect the information soon, but it may take several months for the government to make a decision on whether to reopen the market. We will ask for additional documents if the information doesn't contain enough data to ensure the safety of U.S. beef." MOAF official Park Hyun-chool said if Korean experts agree that U.S. beef is safe to eat, trade representatives of the two countries will meet several times to negotiate sanitary conditions and other safety issues.

Source: http://times.hankooki.com/lpage/biz/200508/kt200508162024221_1910.htm

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

19. *August 16, Reuters* — Dutch to keep poultry indoors to prevent bird flu. The Dutch Agriculture Ministry decided on Tuesday, August 16, to make farmers keep all poultry indoors to prevent contact with migrating birds that could spread bird flu found in Russia. There are concerns that the virus could spread westward to Europe, Middle East, and Africa as tens of millions of birds continue their migration to warmer climates from next month ahead of Russia's harsh winter. "Agriculture Minister (Cees) Veerman will soon announce a package of measures to prevent bird flu reaching the Netherlands," the Dutch ministry said in a statement. "These... include keeping industrial poultry indoors." A relatively small part of the some 105 million poultry in the Netherlands, one of the world's biggest meat exporters, are kept outdoors for animal welfare reasons. But a special bird flu commission of Dutch virologists and veterinarians, set up to advise the ministry on how to prevent the disease said there was a danger that infected migrating birds could spread the deadly disease to outdoor poultry. Senior Russian agricultural officials believe the deadly H5N1 strain was brought by migrating birds from Asia, where more than 50 people have died from that strain since 2003.

Source: http://today.reuters.com/News/CrisesArticle.aspx?storyId=L16_696375

20. *August 16, Reuters* — U.S. seeks massive stock of smallpox vaccine. The U.S. has issued a tender for up to 80 million doses of a smallpox vaccine to guard against terrorist attack, worth over one billion dollars, vaccine-makers said on Tuesday, August 16. The U.S. has been building vaccine stocks ever since the discovery of anthrax spores in its mail system in 2001 sparked fears of a major bioterrorist assault. "The U.S. government plans to procure a stockpile of MVA as part of its defense against the threat of smallpox virus being used as a bioterrorist weapon," Britain's Acambis said of its weakened MVA vaccine. The weakened version is designed for the elderly and patients with immune disorders and skin conditions such as

eczema. Acambis said the U.S. tender was for 20 million doses of the weakened MVA vaccine in the first two years, with the option of a further 60 million doses later on. The U.S. has already stockpiled more than 180 million doses of full strength vaccine against smallpox.

Source: <http://today.reuters.com/business/newsArticle.aspx?type=health&storyID=nL16670027>

21. *August 15, McClatchy Newspapers* — Washington state officials watch for flu pandemic.

Every morning a dozen or so staffers at the Tacoma–Pierce County Health Department in Washington state get together to review hospital emergency room and ambulance call records from the previous 24 hours. It's part of the department's surveillance effort to detect infectious diseases. During the winter, a spike in flu–type cases could signal the outbreak of the actual flu season or that people were getting sick from eating a bad batch of cottage cheese. And as health officials worldwide warn of a global outbreak of avian influenza, the department's early–warning system could offer the first indication the disease has arrived locally. Though avian flu has, so far, been confined to Asia, health officials in Washington state are taking the threat seriously. Because it is a gateway to and from Asia, the Pacific Northwest could be one of the first regions in the U.S. affected. More than 1,200 people arrive daily at Seattle–Tacoma International Airport from Asia. Another 900 land in Portland, OR, and 4,000 more at Vancouver, Canada. Ships from the Far East call at the ports of Tacoma and Seattle. The West Coast could also be a gateway for the geese, ducks, and other migrating birds that carry avian flu.

Source: <http://www.knoxstudio.com/shns/story.cfm?pk=PANDEMIC-WEST-08-15-05&cat=AN>

22. *August 11, University of Pennsylvania* — Researchers discover key to how Severe Acute Respiratory Syndrome virus infects cells. Researchers from the University of Pennsylvania School of Medicine have found that inhibitors of an enzyme called cathepsin L prevent the Severe Acute Respiratory Syndrome (SARS) virus from entering target cells. This study also demonstrates a new mechanism for how viral proteins are activated within host cells, said Paul Bates, senior study author. To gain entry, a virus binds to receptors on the surface of the host cell, and is taken up into a vesicle, or sphere, inside the cell. Unlike most known viruses, the SARS coronavirus needs one more step to infect the cell. The proteins within the membrane of SARS need to be cut by special cellular enzymes (cathepsins) in order to replicate within the host cell. Cathepsins act in the low pH (acidic) environment inside the vesicle, facilitating fusion of the viral membrane and the vesicle membrane, so that viral proteins and nucleic acids can enter the cell where viral replication occurs. “This paper changes the thinking of the field,” says Bates. This gives us a new target to address in the development of therapeutics against the SARS virus.” The researchers found that several chemical inhibitors of cathepsin activity blocked infection of human cell lines by the SARS virus.

Source: http://www.uphs.upenn.edu/news/News_Releases/aug05/SARS.htm

23. *August 11, Yale University* — Animal disease as an early warning system. Yale School of Medicine has launched a database containing scientific evidence about how animal disease events can be an early warning system for emerging human diseases. There have long been reports of animals succumbing to environmental hazards before humans show signs of illness, according to the project's leader, Peter Rabinowitz. "This concept of a 'canary in a coal mine' suggests that animals may be useful sentinels for human environmental health hazards," said

Rabinowitz. He points to the practice in the U.S. and Britain where coal miners would bring canaries into coal mines as an early warning signal for carbon monoxide and other poisonous gases. The birds, being more sensitive, would become sick before the miners. Rabinowitz said several episodes of illness in animals have been clearly linked to human health threats, including cats and mercury poisoning, and wild bird mortality and West Nile Virus infection. Rabinowitz said non-human animals could be more sensitive to many of the agents that are potential biological or chemical weapons and could therefore serve as “sentinels” for a terrorist attack. The Canary Database of Animals as Sentinels of Human Environmental Health Hazards, is a web-based collection of animal sentinel studies that have been collected and curated in terms of their relevance to human health.

Canary Database: <http://canarydatabase.org>

Source: <http://www.yale.edu/opa/newsr/05-08-11-01.all.html>

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

24. *August 16, The Pueblo Chieftain (CO)* — Security network nearing completion in Colorado.

Colorado is very close to linking all of its first responders together with an 800 MHz radio network, and future federal homeland security grants should help complete that link, according to Mike Beasley, director of the state's Department of Local Affairs. According to Beasley, 95 percent of the state will be linked to the 800 MHz network in the next year. Toward that goal, restrictions have been set in Colorado on new grant applications — no grants will be awarded for communication equipment that does not connect to the 800 MHz system.

Source: <http://www.chieftain.com/metro/1124200807/2>

25. *August 16, Cincinnati Business Courier (OH)* — Kentucky is first state to complete security requirement. The Kentucky Office of Homeland Security was told by the Department of Homeland Security (DHS) that Kentucky is the first state in the nation to complete the National Incident Management System Capability Assessment Support Tool (NIMCAST), the first step in a process to reaching full National Incident Management System, or NIMS, compliance. The NIMS was established by DHS to provide a consistent nationwide template to enable all government, private-sector and nongovernmental organizations to work together during domestic incidents. NIMS compliance is a prerequisite to obtaining most federal preparedness funding. The NIMCAST is a web-based, self-assessment system that state agencies and local jurisdictions used to evaluate their incident response and management capabilities. It also identifies how compliant an agency is with federal incident management guidelines.

Source: http://www.bizjournals.com/cincinnati/stories/2005/08/15/daily11.html?from_rss=1

26. *August 15, NBC 17 (NC)* — Army, North Carolina authorities stage terrorism response drill. Almost four years after 9/11, commanders at Fort Bragg, NC, staged the largest drill in

state history Monday, August 15, to prepare for a future terrorist attack on American soil. Operation Orbit Comet simulated the response to several Congressmen being taken hostage by terrorists. An unknown number of troops, local law enforcement and community leaders worked together in the drill. "The coordination it takes to pull this off creates, again, some building blocks that we continually step up as we climb up the mountain trying to understand where our country's vulnerabilities are," said Major General Virgil Packett, the Army base's interim commander. The exercise continues through Friday, August 19, with other simulated events, such as a safe-house raid, the detonation of a large explosive device on a ferry and a simulated commercial oil spill at the State Port in Morehead City, NC. Other simulated exercises include a computer exercise involving a pneumonic plague and a rail line chlorine incident.

Source: http://www.nbc17.com/news/4854161/detail.html?rss=tri&psp=ne_ws

27. *August 15, News-Miner (AK)* — Drills test response to major emergency in Alaska.

Elaborate drills to test the Alaska's ability to respond to terrorist attacks and natural disasters are planned in 21 communities throughout the week. Alaska routinely conducts emergency response drills, but the coming week's exercises are more complex, more numerous and involve more people and locations than ever before, said Jamie Littrell, spokesperson for the Alaska Division of Homeland Security and Emergency Management. Nearly 5,000 people from various government agencies are expected to participate in the training. The main Fairbanks, AK, drill will be held Tuesday, August 16, at 2 a.m. at the Fairbanks International Airport and concerns three simulated events, a release of hazardous materials, a terrorist incident and a mass casualty episode, according to Barry Jennings, emergency operations manager for the Fairbanks North Star Borough. Exercises are also planned at the University of Alaska-Fairbanks (UAF) and the Flint Hills Resources Alaska refinery. UAF's drill is planned for Thursday, August 18, and whether it will be terrorist related or a natural disaster has not been released. The campus enlisted the help of the National Guard 101st Civil Support Team from Idaho for the drill. A drill is also planned at the Alaska-Canada border.

Source: <http://www.news-miner.com/Stories/0,1413,113~7244~3010865,00.html>

[[Return to top](#)]

Information Technology and Telecommunications Sector

28. *August 16, US-CERT* — Vulnerability Note VU#896220: Adobe Acrobat contains a remotely exploitable buffer overflow. Adobe Acrobat is a suite of applications that allow users to manipulate PDF (Portable Document Format) files. A buffer within a core plug-in for Adobe Acrobat and Acrobat Reader can be overwritten using a specially-crafted PDF document. If a remote attacker can persuade a user to access a specially crafted PDF file, that attacker may be able to execute arbitrary code or crash the Adobe Acrobat/Acrobat Reader process. Users should upgrade to unaffected versions of Adobe Acrobat and Acrobat Reader. For a list of unaffected versions please see Adobe Security Advisory 321644:

<http://www.adobe.com/support/techdocs/321644.html>

Source: <http://www.kb.cert.org/vuls/id/896220>

29. *August 16, Techtree* — Apple releases OS X patches. Apple has released a security update for Mac OS X, which addresses several potential vulnerabilities in the operating system. The

update incorporates patches for AppKit, which prevent malicious users from executing malware stored in carefully crafted, rich-text files. The Bluetooth code is modified, to ensure that devices' requirement for an authenticated connection is reported correctly. The security update also fixes "algorithmic complexity attack" vulnerabilities in the OS' CoreFoundation code. The update includes patches for the Directory Services code as well. Kerberos has been updated to version 5.5.1, which prevents multiple buffer overflows resulting in remote compromise of a KDC or denial of service. The Loginwindow application which handles user accounts, has been repaired to prevent a local user who knows the password for two accounts, from being able to log into a third account without knowing the password. Safari is patched to prevent arbitrary command execution, as also sending of information submitted in a form to the wrong Website. As of now, two updates are available, one for Mac OS X 10.4.2 and the other for 10.3.9. Both are further sub-divided into server and client versions.

Apple Website: <http://docs.info.apple.com/article.html?artnum=61798>

Source: http://www.techtree.com/techtree/jsp/article.jsp?article_id=5484&cat_id=582

30. *August 15, Security Focus* — **CPAINT unspecified command execution and information disclosure vulnerabilities.** CPAINT is affected by unspecified command execution and information disclosure vulnerabilities. These issues are most likely due to an access validation error. Successful exploitation of these vulnerabilities could lead to a compromise of the server running the affected application. Information obtained may also aid in further attacks; other attacks are also possible. The vendor has addressed this issue in the latest release of the software.

CPAINT Upgrade `cpaint-v1.3-SP.tar.gz`:

<http://prdownloads.sourceforge.net/cpaint/cpaint-v1.3-SP.tar.gz?download> ad

Source: <http://www.securityfocus.com/bid/14565/references>

31. *August 15, FrSIRT* — **phpMyFAQ XML-RPC for PHP Nested Tags Remote Code Execution.** A vulnerability was identified in phpMyFAQ, which could be exploited by remote attackers to execute arbitrary code. This flaw is due to an input validation error in the XML-RPC library when processing, via an "eval()" call, certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. Affected products include phpMyFAQ version 1.4.10 and prior, and phpMyFAQ version 1.5.0-RC6 and prior. Users should upgrade to phpMyFAQ version 1.4.11:

<http://www.phpmyfaq.de/download.php>

Source: <http://www.frsirt.com/english/advisories/2005/1416>

32. *August 15, FrSIRT* — **Drupal XML-RPC for PHP nested tags remote code execution.** A vulnerability was identified in Drupal, which could be exploited by remote attackers to execute arbitrary code. This flaw is due to an input validation error in the XML-RPC library when processing, via an "eval()" call, certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. Affected products include Drupal version 4.6.0 through 4.6.2 and Drupal version 4.5.0 through 4.5.4. Users should upgrade to Drupal version 4.5.5 or 4.6.3:

<http://drupal.org/project>

Source: <http://www.frsirt.com/english/advisories/2005/1415>

33. *August 15, Security Focus* — **PHPXMLRPC and PEAR XML_RPC remote code injection vulnerability.** PHPXMLRPC and PEAR XML_RPC are affected by a remote PHP code

injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary server-side script code on an affected computer with the privileges of the Web server process. This may facilitate unauthorized access. The vendor has released version 1.2 of PHPXMLRPC and version 1.4 of PEAR XML_RPC to correct this problem. Nucleus CMS has released a patch addressing this issue. Reports indicate an upgrade will be available shortly. Please contact the vendor for further information.

Source: <http://www.securityfocus.com/bid/14560/references>

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of actively propagating worm variants, known as Zotob.A and Zotob.B. The initial worm variant was released into the wild on August 14, 2005. Both variants exploit the Microsoft Windows Plug and Play vulnerability (MS05-039). Once infected, the victim opens a backdoor shell on port 8888/TCP, establishes a connection with command and control server(s), and starts an FTP server listening on port 33333/TCP. Zotob infected systems scan their local class B (/16 CIDR) network block for port 445/TCP and exploit the vulnerability within MS05-039 to propagate. If successful, the newly exploited system reaches back to the infect system and downloads the worm via FTP over port 33333/TCP.

The following hostnames have been identified as Zotob Command and Control servers:

diabl0.turkcoders.net:8080

wait.atillaekici.net:8080

real.atillaekici.net:8080

l33t.freeshellz.org:5232

IMPACT: Successful exploitation will result in port 445/TCP scanning and further propagation to other vulnerable systems within the local class B network block. Additionally, the exploitation may result in the execution of arbitrary code through the backdoor or Internet Relay Channel (IRC) Command and Control channel.

RECOMMENDATIONS: Please apply the patches identified within MS 05-039, and update to the latest anti-virus signatures. Additional recommendations are to:

* Disable NULL sessions (NULL sessions are disabled by checking the registry entry HKLM\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymoussam, ensuring it is enabled.

* Block port 445/TCP at the network boundaries * Monitor the network for port 445/TCP scanning * Monitor the network for unauthorized or suspicious outbound port 8080/TCP connections and monitor connections to any of the hostnames previously mentioned.

SYSTEMS AFFECTED: Microsoft Windows 2000, XP Zotob variants will run on but not infect 95/98/Me/NT4. The variants will not propagate to default installs of MS Windows XP SP2 or 2003 because NULL sessions are disabled by default.

Current Port Attacks

Top 10 Target Ports	445 (microsoft-ds), 1026 (----), 1433 (ms-sql-s), 135 (epmap), 1234 (hotline), 6346 (gnutella-svc), 139 (netbios-ssn), 4672 (eMule), 50000 (SubSARI), 1434 (ms-sql-m) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[[Return to top](#)]

General Sector

34. *August 15, Reuters* — **Italy arrests 141 in terror sweep.** Italy has arrested 141 people in a security sweep following the bombings in London, England, and Egypt last month and remains at high risk from an attack by Islamic militants, the Interior Ministry said on Monday, August 15. Italy, the subject of several Internet threats from purported Islamic militant groups, said it had begun expulsion procedures against 701 people. "The latest evaluations ... confirm an ongoing high risk of a terrorist attack on our country," the ministry said in a statement after a parliamentary meeting on the findings from a series of nation-wide raids in recent days. Nearly 33,000 people had been questioned in recent days as part of the nation-wide investigation that involved all branches of Italy's security and police forces, the ministry said. Owners of money transfer agencies, call centers, and Internet cafes had been investigated and two of the people arrested were brought in under newly-approved anti-terror laws, it added. Parliament last month passed measures that give the Italian state greater powers to combat terrorism after Interior Minister Giuseppe Pisanu said terrorists were "knocking on Italy's door."

Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=topNews&storyID=2005-08-15T141459Z_01_MOL551274_RTRUKOC_0_UK-SECURITY-ITALY.xml

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.